Hogan Lovells

Study of proposal for an ePrivacy Regulation

November 2019

Mastering Digital

Contents

1. Introduction and background

1.1 On 10 January 2017, the European Commission issued a proposal for a new ePrivacy Regulation (**ePR**)[1] triggering a legislative process that is still ongoing. The proposed ePR was intended to replace the existing ePrivacy Directive 2002/58.[2] As well as updating the current ePrivacy framework in the EU, the Commission has qualified the proposal as lex specialis to the General Data Protection Regulation 2016/679 (**GDPR**), which it is designed to "complement and particularise."[3] With this in mind, the original aim had been for the proposed ePR to become enforceable on 25 May 2018 (at the same time as GDPR).

1.2 Following the publication of the proposed ePR, the European Parliament adopted its report[4] with the mandate for entering into inter-institutional negotiations in October 2017. However, the Council of the European Union has not yet been able to agree its position. The Council has been seeking better alignment of the proposed ePR with the GDPR and to find solutions on many open questions. After two and a half years of negotiations, it remains uncertain whether a Common Approach can be reached.

1.3 During the nearly three years since the proposed ePR was issued, many amendments have been suggested and debated in the Council with a view to solving the concerns raised by Member States. These amendments have sought to achieve the right balance between the need for technological innovation, public security and the protection of privacy in the context of the digital economy. The structure of the proposed ePR and the way in which it was originally construed, however, have made a suitable way forward difficult to find.

1.4 This study aims to provide a critical evaluation of the proposed ePR. It is by no means an exhaustive analysis but looks at some of the aspects that have proven to be in conflict with the approach of the GDPR and the various objectives behind the proposal.[5] This study also aims to formulate some essential public policy suggestions for a new text which supports the objectives of the proposed ePR in a more pragmatic and feasible way, avoiding the legal uncertainty created by some foundational elements of the current proposal.

Eduardo Ustaran
Partner, London
+44 20 7296 5249
eduardo.ustaran@hoganlovells.com

2. Executive summary

When updating the EU ePrivacy framework, a balance needs to be struck between the protection of privacy and public security in the context of the digital economy and the need for technological development. This balance needs to be effective in practice and aligned with the existing framework for the protection of personal data, which is closely related to the protection of confidentiality.

Our critical evaluation of the proposed ePR has shown that:

- Rather than complementing the GDPR, the current proposal is in some respects in conflict with the basic tenets of the EU data protection framework.
- The essence of flexibility in the application of the GDPR created by focussing on risk is fundamentally missing from the proposed ePR, which instead imposes a general prohibition on processing with narrow exceptions. This creates a dual and conflicting system in which standards for the protection of personal data are not consistently applied.
- The rules covering the confidentiality of communications have grown in complexity as the legislators sought ways to avoid situations where specific desirable use cases were not permitted by law. The result is unlikely to be optimal, given the breadth of processing activities covered, unless elements of the GDPR's risk-based approach are introduced.
- The close relationship between Articles 7 and 8 of the Charter of Fundamental Rights of the European Union emphasises and demonstrates the fact that the protection of the right to respect for private life, which the proposed ePR is specifically seeking to protect with regard to communications, needs to be compatible with the mechanisms of protection set out in the GDPR.

In light of our critical analysis and findings, a number of essential steps are recommended to improve the text. In particular:

- The ePR should **move away from an approach that protects confidentiality predominantly, if not exclusively, by setting out specific legal bases** for the processing of specific types of data.
- By contrast, a **risk-based approach** should be applied with the introduction of a similar **"balancing test"** as under the GDPR's Article 6(1)(f), applying to activities that cause little or no privacy impact. This will allow **proportionality and accountability** based on the risks of the associated data processing.
- Data **processing that poses no risks to individuals, such as data that is or is made anonymous, should be explicitly excluded** from the ePR's scope, which in line with the GDPR should only apply to personal data. This will be particularly important in an IoT context, where data relating to machines will lack any personal identifiers.

Overall, our analysis shows that improvements to the text are possible only if a reconsideration of the proposal's core approach to regulating the legal bases for processing is undertaken.

3. Critical analysis of the current proposal for an ePrivacy regulation

(A) Overview of the Proposed ePR

3.1 The proposed ePR has 43 Recitals, 7 Chapters and 29 Articles. At a high-level:

- **Chapter I** sets out the material and territorial scope of the proposed ePR and defines various terms used. While definitions are borrowed from the GDPR and the European Electronic Communications Code (EECC),[6] they are expanded to include "ancillary features" under the definition of "interpersonal communications service" as well as non-personal data under the definition of "processing."[7]
- **Chapter II** focuses on the protection of end-users' electronic communications (comprising the two categories of content data and metadata as well as rules on storage and erasure) and the integrity of their terminal equipment (comprising the two categories of information "collected from" and "emitted by" terminal equipment). Different sets of legal bases (for a total of 22) and conditions are set out separately for each category of data. New consent requirements compared to the ePrivacy Directive are set out for the processing of content and metadata by service providers. Separate rules and conditions are also set out for the compatible processing of metadata and for detection of child sexual abuse material.
- **Chapter III** sets out specific obligations for number-based interpersonal communications services, traditionally applicable to telecoms operators, concerning calling line identification, the prevention of unwanted calls and publicly available directories. It also sets out rules preventing direct marketing by any individual or organisation unless the end-user has consented or when such communications happen in the context of a purchase of a product or a service.
- **Chapter IV** sets out the possibility for Member States to designate one or more competent authority for the ePR's enforcement – which can include not only Data Protection Authorities (DPAs), who are responsible for the GDPR, but also National Regulatory Authorities (NRAs) responsible for telecoms regulation. The European Data Protection Board (EDPB) is entrusted to "contribute to" the ePR's consistent application (as opposed to "ensure" in the original Commission proposal), establishing only a general duty to cooperate between the competent authorities not subject to the GDPR's consistency mechanism.[8]
- **Chapter V** provides for remedies, liability and penalties. It sets out administrative fines for infringements of specific provisions up to 4% of total worldwide annual turnover, which can apply concurrently to GDPR penalties.[9]
- **Chapters VI** and **VII** set out the rules for the adoption of delegated acts, where the Commission will be assisted by the Communications Committee, responsible for the European Electronic Communications Code (EECC), as opposed to the Committee responsible for the GDPR.[10]

3.2 To summarise, the proposed ePR seeks to provide for the confidentiality of electronic communications data and terminal equipment data by defining specific and limited situations in which processing of such data is permitted.

3.3 For the purposes of this analysis, the key focus is on the provisions dealing with electronic communications data and terminal equipment, as these provisions are at the core of the current legislative debate and present the greatest challenge to meet the proposal's policy aim.

(B) Analysis of the proposed ePR's electronic communications data provisions

3.4 The proposed ePR's Explanatory Memorandum makes it clear that the proposal is intended to build upon and complement the existing structure of the EU's data protection and telecoms frameworks, ensuring that areas where there is a genuine legislative gap are adequately dealt with to protect users' privacy.

3.5 The confidentiality of electronic communications does indeed involve considerations which are not specifically addressed in the GDPR. Complementary provisions with respect to these processing activities may, therefore, be appropriate. However, the proposed ePR tackles confidentiality predominantly by replacing the legal bases for processing available under the GDPR with new sets of legal bases depending on the category of data at hand. This approach is narrow and causes tensions with key features of the GDPR, as further explained below.

Complexity and inconsistency in the legitimacy of data uses

3.6 The GDPR's Article 6 allows for six lawful grounds for data processing, all of which have equal status. This provides a pragmatic approach to the legitimacy of the processing of personal data.

3.7 In contrast to this approach, the proposed ePR (Article 6, which the Council has split into six articles, from 6 to 6d) establishes a general prohibition to the processing of electronic communications data, except when permitted under one of its legal bases, which vary for electronic communications content and electronic communications metadata. In the original Commission proposal, such exceptions, depending on the type of data at hand, are essentially linked to: the mere transmission of communications (Article 6(1)(a)); network and service security (Article 6(1)(b)); service provision subject, in addition, to end-user consent (Article 6a(1)(a)); consent of the end-users involved in the communication for specific purposes (Articles 6a(1)(b) and 6b(c)); network management/optimisation (Article 6b(a)); and billing (Article 6b(b)).

3.8 The diverse use cases and types of data processing that could be covered as electronic communications data, going beyond the traditional use cases covered under the telecoms-related legal bases illustrated above, show that an approach that relies on a blanket prohibition qualified by limited exceptions is likely to lead to unwanted effects.

3.9 The resulting framework covering the general confidentiality of communications has grown in complexity, as the legislators sought ways to avoid situations where specific desirable use cases could be identified but could not be accommodated under one of the originally proposed legal bases. This has included taking into account: expanding the scope of Article 6(1)(a) beyond transmission to cover service provision as a whole; improving device security (Article 6(1)(c)) as opposed to the sole security of networks and services; compliance with a legal obligation (Article 6(1)(d)); traffic management and optimisation (Article 6b(a)) as opposed to mandatory quality of service; the protection of vital interests (Article 6b(d)), statistical purposes and scientific research (Article 6b(f)); compatible purposes (limited to metadata under Article 6c, which in addition to restating those contained in the GDPR lists another five conditions); and the detection of child abuse material (with specific rules contained in Article 6d).

3.10 The narrow scope allowed by the proposed exceptions does not allow for nuance in the array of processing activities which fall within the scope of the proposed ePR and undermines the complexity of electronic communications. This is a clear handicap for a piece of legislation that relates to a constantly evolving sector. As well as potentially damaging its long-term relevance and effectiveness, this creates an obvious conflict between the approach taken by the GDPR, which allows the lawful bases and legitimacy for processing to be interpreted in a context-specific manner, and the proposed ePR, which treats all in-scope processing activities as high-risk.

3.11 This conflict is particularly evident in the context of evolving communications and digital technology. At present, the development of machine-to-machine (M2M) communications, Internet of Things (IoT) devices and services, and artificial intelligence (AI) relies on the ability to retrieve and use data which is likely to be regarded as electronic communications data under the proposed ePR.[11] The use of AI, which is an essential part of the Commission's strategy to digitise industry and society, is crucially dependent on access to electronic communications data.[12]

3.12 As a result, the protection of electronic communications data should be achieved by ensuring that any additional layer of regulation applicable to it is compatible and consistent with the GDPR. The conditions for data processing set out in Article 6 of the GDPR for personal data and in Article 9 of the GDPR for special categories of personal data need not be undermined, as they provide a tried and tested ground for the use of data which is also suitable in the context of electronic communications.

3.13 This is further reinforced by the relationship between Articles 7 and 8 of the Charter of Fundamental Rights of the European Union (the "Charter"). The Court of Justice of the European Union has repeatedly stated that the right to respect for private life (under Article 7 of the Charter) is closely connected with the right to the protection of personal data (under Article 8 of the Charter).[13] This close relationship emphasises and demonstrates the fact that the protection of the right to respect for private life, which the proposal is specifically seeking to protect with regard to communications, needs to be compatible with the mechanisms of protection set out in the current framework dealing with the protection of personal data, and more specifically the GDPR.

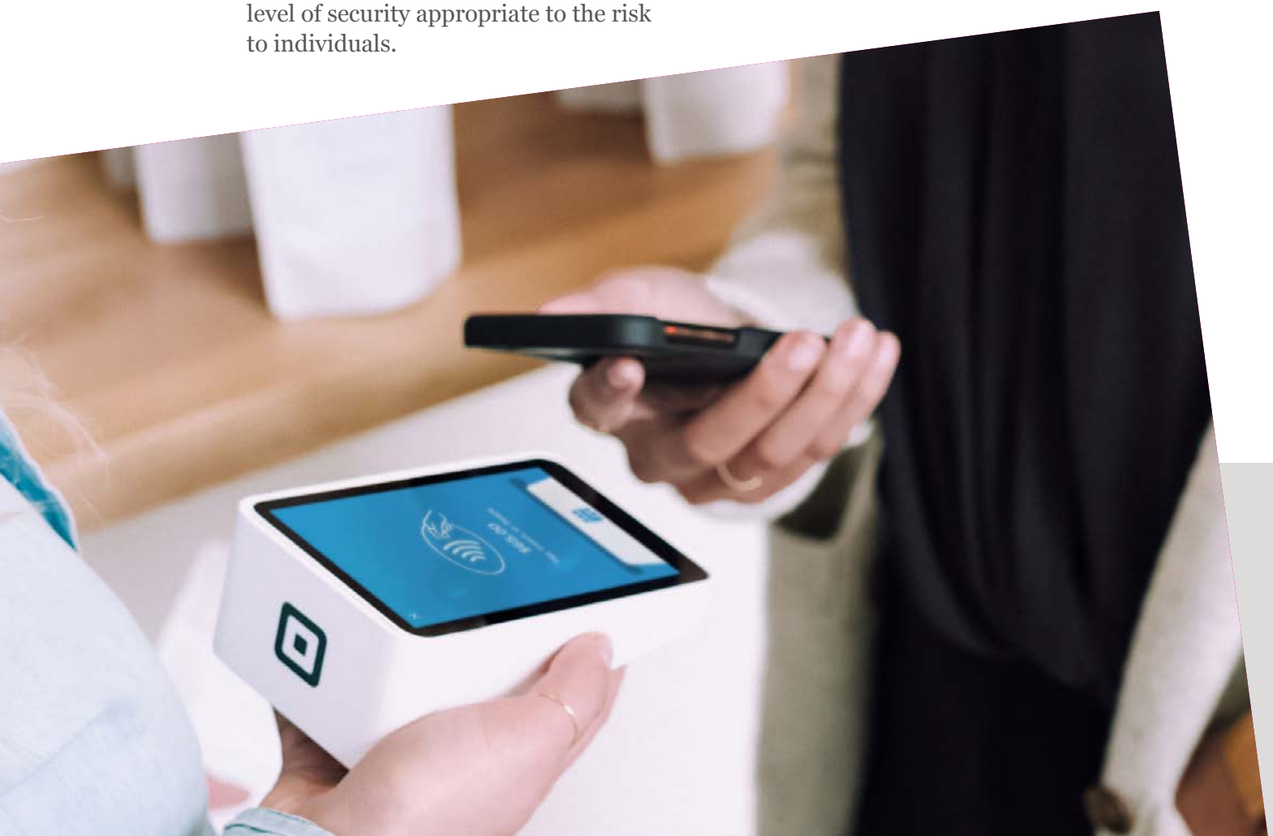
The loss of the GDPR's risk-based approach

3.14 As indicated in the GDPR's recitals, risk in a data protection context is an objective assessment determined by considering the nature, scope, context and purposes of the processing.[14] This creates flexibility and, by being context-specific, allows for the same legal framework to adapt and apply to a myriad of processing activities, situations and risks.

3.15 A consideration of risk is enshrined throughout the GDPR and the word "risk"/"risks" can be seen in use in many of its key provisions, including most significantly:

- Article 6(1)(f) enables organisations to process personal data based on their legitimate interest after conducting a risk-based assessment of how that processing will affect the rights and freedoms of individuals.
- Articles 24 and 32 allow controllers and processors to implement technical and organisational measures to ensure compliance with the regulation and a level of security appropriate to the risk to individuals.
- Articles 33 and 34 allow a controller to assess whether or not a breach is worthy of reporting to the relevant DPA and data subjects based on the level of risk posed to those data subjects.
- Article 35 allows a controller to determine whether a data protection impact assessment is required for a particular processing activity depending on the risk to individuals.

3.16 Given that the proposed ePR is intended to be read alongside the GDPR, some of these risk-based GDPR provisions will of course still apply to the processing of electronic communications data. Nonetheless, a fundamental component of such flexibility in the application of the law is missing in the proposed ePR, namely the ability to identify the most appropriate legal bases in a manner that is proportionate to the risks of the associated data processing. Again, this creates a dual and conflicting system in which standards for the protection of personal data are not consistently applied.



(C) Analysis of terminal equipment provisions

3.17 Similarly to the situation regarding electronic communications data, the terminal equipment provisions in the proposed ePR, which include separate rules pertaining to information "collected from" (Article 8(1)) and "emitted by" (Article 8(2)) terminal equipment, are in conflict with the approach taken in the GDPR for the following principal reasons:

- The complexity of the data uses covered.
- The loss of the GDPR's risk-based approach.

We explain each of these points in more detail below.

Complexity of data uses covered

3.18 Article 8(1) of the proposed ePR is drafted widely, and includes *"processing and storage capabilities of terminal equipment and the collection of information from end-users' terminal equipment, including about its software and hardware."* This scope is wider than that currently covered by the ePrivacy Regulation (Article 5(3)), which is limited to *"the storing of information, or the gaining of access to information already stored"* in terminal equipment. Contrary to the current ePrivacy Directive, the proposed ePR does not only apply to the cookie use case, where data has to be stored on a device, but also to any information about such device.[15] This is particularly noteworthy in the case of IoT devices as any processing of data for the resulting IoT service will be based on data about that device.

3.19 As a consequence, the processing of a broad spectrum of information, including both personal and non-personal data, will be subsumed under the ePR's provisions on terminal equipment, irrespective the actual impact of such processing on secrecy of communications and private life. Moreover, application of the ePR's terminal equipment provisions is not bound by the definition of electronic communications service, which by contrast triggers the application of the electronic communications data provisions. This means that any digital service, even those not qualified as electronic communications services or information society services, will have to implement the ePR's terminal equipment provisions.

3.20 By way of non-exhaustive examples, M2M-, IoT- and AI-related areas that may be adversely affected by this include:

- Research in e-health and the deployment of remote medical services;
- Research and development of safety features in the automotive industry and, in particular, autonomous and self-driving vehicles;
- Monitoring and running of essential services ranging from energy consumption and manufacturing processes to banking and transportation;
- Cybersecurity generally; and
- Research and development of new features and services generally, even based on pseudonymous or anonymous data.

3.21 Similarly to the electronic communications data provisions, the proposed ePR tackles confidentiality predominantly by replacing the legal bases for processing available under the GDPR with new legal bases. It sets out a blanket prohibition to the processing of terminal equipment data followed by a narrow list of exceptions. These essentially relate to: the transmission of electronic communications or the establishment of a connection (Articles 8(1)(a) and 8(2)(a)); the end-user's consent (Articles 8(1)(b) and 8(2)(b)); service provision (Articles 8(1)(c) and 8(2)(d)), which is interpreted strictly;[16] audience measuring limited to information society services or statistical counting (Articles 8(1)(d) and 8(2)(c)); security of information society services and terminal equipment (Article 8(1)(da)); software updates that are necessary for security reasons (Article 8(1)(e)); and determining location for emergency calls (Article 8(1)(f)).

3.22 As we have observed in relation to electronic communications data, the narrow list of permitted processing activities concerning terminal equipment has grown compared to the original proposal from the Commission (11 in the latest text as opposed to 6) to allow specific uses that could be identified during the negotiations. Nevertheless, the list contained in the latest Council text remains narrow and undermines the complexity of the processing activities which fall within the scope of the proposed ePR's terminal equipment provisions.

The loss of the GDPR's risk-based approach

3.23 Misalignment with the GDPR is again particularly noticeable with respect to the form of risk-based assessment set out in the GDPR's Article 6(1)(f). Processing on the basis of a controller's legitimate interests under the GDPR is meant to help prevent overreliance on other legal bases, such as consent, under the right circumstances and subject to adequate safeguards.[17]

3.24 The GDPR's legitimate interest legal basis places an obligation on the controller to weigh whether the interests or fundamental rights and freedoms of the data subject override the controller's legitimate interest. In instances where this "balancing test" shows that the processing is too invasive with respect to the data subject's interests, Article 6(1)(f) cannot be invoked.

3.25 Unlike processing under one of the GDPR's other five grounds, which is considered a priori legitimate, Article 6(1)(f) requires a specific test to be carried out. The use of legitimate interest presents complementary safeguards requiring appropriate measures on the part of controllers and *"aims at a balanced approach, which ensures the necessary flexibility for data controllers for situations where there is no undue impact on data subjects, while at the same time providing sufficient legal certainty and guarantees to data subjects that this open-ended provision will not be misused."*[18] This way, individuals' rights are still protected, including their right to opt out of the processing at any time (Article 21 of the GDPR), but an element of flexibility is introduced.

3.26 To ensure consistency with the GDPR and longevity of the new ePrivacy rules, similar determinations should be allowed through the use of balancing tests in relation to the protection of end-users' terminal equipment. At present, processing that does not fall within Article 8's narrow exceptions but is nonetheless not high-risk, intrusive or potentially harmful cannot rely on any legal basis in the proposed ePR apart from consent (Articles 8(1)(b) and 8(2)(b)). This creates an inherent tension with the need to *"create more specific exceptions, to allow for the processing of data that causes little or no impact on the rights of users to secrecy of communications and private life."*[19]

4. An alternative approach to regulating ePrivacy in the EU

4.1 In a world where electronic communications and devices play an increasingly important role in everyday lives, personal data – including electronic communications and terminal equipment data – becomes increasingly valuable. A clear set of ePrivacy rules which protect the privacy of individuals in harmony with the GDPR is needed to ensure an appropriate balance between protection and beneficial types of data processing.

4.2 Our analysis above has illustrated how the proposed ePR, in the Council version that has tried to accommodate this balance over the course of two and a half years of negotiations, fails to achieve a workable framework that can complement rather than contradict essential elements of the GDPR.

4.3 In light of the critical analysis above and our findings in this respect, the following essential steps should be taken to improve the proposed ePR:

- The text should **move away from an approach that protects confidentiality predominantly, if not exclusively, by setting out specific legal bases** for the processing of specific types of data. Such an approach would work if the scope of processing activities and the types of data covered were more limited. However, the proposed ePR's scope includes many different types of processing operations – under this condition, as highlighted in our analysis, misalignment with the GDPR legal bases becomes more difficult to remedy by expanding the list of narrow exceptions.
- The **valuable risk-based approach of the GDPR should be applied** to the ePrivacy framework. Crucially, this requires the **introduction of a similar "balancing test"** as that allowed under the GDPR's Article 6(1)(f), which allows organisations to identify the most appropriate legal bases in a manner that is proportionate to the risks of the associated data processing.
- **Data processing that poses no risks to individuals, such as data that is or is made anonymous, should be explicitly excluded from the ePR's scope,** which in line with the GDPR should only apply to personal data. This will be particularly important in an IoT context, where data relating to machines will lack any personal identifiers.

4.4 In conclusion, while a balanced ePR should explicitly reinstate the principle of confidentiality of electronic communications, it should also acknowledge that this is not an absolute principle and that any interference with it should be justifiable in accordance with the existing data protection framework, aligned with Articles 7 and 8 of the Charter. Our recommendations stem from a basic analysis of the proposed ePR as originally put forward by the European Commission and subsequently modified in Council negotiations. Our analysis shows that improvements to the text are possible provided a reconsideration of the proposal's core approach to regulating the legal bases for processing is undertaken.

References

1. Proposal for a Regulation of the European Parliament and the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications) COM(2017) 10 final
2. As modified by Directives 2006/24/EC and 2009/136/EC
3. Recital 5 proposed ePR
4. Draft European Parliament Legislative Resolution on the proposal for a regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications) (COM(2017)0010 – C8-0009/2017 – 2017/0003(COD))
5. Our analysis focuses on the discussions in the Council of the EU specifically and is based on the latest consolidated text circulated by the Finnish Presidency, doc. 14054/19
6. Directive (EU) 2018/1972 of the European Parliament and of the Council of 11 December 2018 establishing the European Electronic Communications Code (Recast)
7. Article 4(2) of the proposed ePR
8. Chapter VII of Regulation (EU) 2016/679
9. Article 83 GDPR
10. Article 93 GDPR
11. See Härting Rechtsanwälte PartGmbB, Study on the Impact of the Proposed ePrivacy Regulation, October 2017, available at https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/epr_-_gutachten-final-4.0_3_.pdf
12. See Communication from the Commission to the European Parliament, the European Council, the Council, the European Economic and Social Committee and the Committee of the Regions on Artificial Intelligence for Europe COM(2018) 237 final.
13. C 92/09 and C 93/09 *Volker und Markus Schecke and Eifert*, paragraph 47; C-468/10 and C-469/10 *ASNEF v Administración del Estado*, paras. 41 and 42; and C-291/12 *Schwarz v Stadt Bochum*, paragraph 26
14. Recital 76 GDPR
15. See Article 29 Working Party Opinion 03/2016 on the evaluation and review of the ePrivacy Directive (2002/58/EC)
16. See most recently the draft EDPB Guidelines 2/2019 on the processing of personal data under Article 6(1)(b) GDPR in the context of the provision of online services to data subjects. The Council has tried to clarify the applicability of this legal basis in the IoT context by adding text in Recital 21 that explicitly mentions a few IoT use cases such as connected thermostats, connected medical devices, smart meters or automated and connected vehicles. This, however, does not change the application of the legal basis itself, which only applies to data that is, in the words of the EDPB, “useful but not objectively necessary for performing the … service … even if it is necessary for the controller’s other business purposes” (ibid. page 8)
17. Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC
18. Ibid., p. 10
19. Article 29 Working Party Opinion 03/2016 on the evaluation and review of the ePrivacy Directive (2002/58/EC), p. 11

Alicante
Amsterdam
Baltimore
Beijing
Birmingham
Boston
Brussels
Budapest*
Colorado Springs
Denver
Dubai
Dusseldorf
Frankfurt
Hamburg
Hanoi
Ho Chi Minh City
Hong Kong
Houston
Jakarta*
Johannesburg
London
Los Angeles
Louisville
Luxembourg
Madrid
Mexico City
Miami
Milan
Minneapolis
Monterrey
Moscow
Munich
New York
Northern Virginia
Paris
Perth
Philadelphia
Riyadh*
Rome
San Francisco
Sao Paulo
Shanghai
Shanghai FTZ*
Silicon Valley
Singapore
Sydney
Tokyo
Ulaanbaatar*
Warsaw
Washington, D.C.
Zagreb*

*Our associated offices
Legal Services Centre: Berlin

www.hoganlovells.com